UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/941,229	08/28/2001	Patrick J. McLampy	050115-1050	5275

24504 7590 06/23/2006

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, LLP
100 GALLERIA PARKWAY, NW
STE 1750
ATLANTA, GA 30339-5948

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 06/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/941,229	MELAMPY ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *45-67 and 70-73* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *45-67 and 70-73* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on 4/14/2006. Claims 45, 52, 59, 60, and 67 are amended. Claims 45-67 and 70-73 are pending.

Response to Arguments

Applicant's arguments, see Remarks sections b and c, filed 4/14/2006, with respect to the rejection(s) of claim(s) 63-67 and 70-73 under U.S.C. 102(e) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Fink et al., (U.S. Patent No. 6,826,684) and Akiyama et al., (U.S. Patent No. 5,623,548).

Applicant argues that Fink et al. fails to teach, disclose or suggest at least "re-sequencing the series of multi-media data flow packets into a pseudo-random order; and transmitting each multi-media data flow packet in the re-sequenced series in the pseudo-random order" as recited in amended claims 45, 52, and 59.

Examiner responds that Fink discloses "the encrypted portions of the packet header are those portions relating to the source and destination hosts 31, and 34 and packet sequencing information ... the receiving ASD peer 35 **restores** packet in accordance with a prearranged protocol. The result of this process is a restored packet identical to the original packet created by the sending host" – Note that such restoration is required because packet header information such as sequence number has been randomized/encrypted before transmission)(col. 7, lines 1-26 and col. 9, lines 30-42).

Fink also discloses "the ASD technique seemlessly layers with data security technologies such as IPSEC and Secure Socket Layer (SSL) because it only affects addressing and sequencing information for translation/restoration, allowing it to be used to enhance existing network security systems" (col. 7, lines 1-15 and col. 9, lines 13-65).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 45-62 are rejected under 35 U.S.C. 102(e) as being anticipated by Fink et al., (U.S. Patent No. 6,826,684 and Fink hereinafter).

Regarding claims 45 and 52, Fink discloses a method of encrypting multi-media data flow packets, comprising the steps of:

receiving a series of multi-media data flow packets, each packet comprising a sequence number, storing the series of multi-media data flow packets in a jitter buffer (i.e., for the duration of translation process, packets have to be stored in some sort of buffer or temporary storage), re-sequencing (i.e., encrypting) the series of multi-media data flow packets into a pseudo-random order (i.e., the encrypted portions of the packet header are those portions relating to the source and destination hosts 31, and 34 and packet sequencing information ... the receiving ASD peer 35 restores packet in accordance with a prearranged protocol. The result of this process is a restored packet identical to the original packet created by the sending host – Note that such restoration is required because packet header information such as sequence number has been randomized/encrypted before transmission)(col. 7, lines 1-26 and col. 9, lines 30-42), and transmitting each multi-media data flow packet in the re-sequenced series (col. 6, lines 19-67 and col. 7, lines 1-67 and col. 9, lines 13-29).

Regarding claim 59, Fink discloses a system for encrypting multi-media data flow packets, comprising:

a transceiver, software stored within said first endpoint defining functions to be performed by the system (col. 6, lines 19-60); and

a processor configured by said software to perform the steps of: receiving a series of multi-media data flow packets, each packet comprising a sequence number, storing the series of multi-media data flow packets in a jitter buffer (i.e., for the duration of translation process, packets have to be stored in some sort of buffer or temporary

storage), re-sequencing (i.e., encrypting) the series of multi-media data flow packets into a pseudo-random order (i.e., the encrypted portions of the packet header are those portions relating to the source and destination hosts 31, and 34 and packet sequencing information ... the receiving ASD peer 35 restores packet in accordance with a prearranged protocol. The result of this process is a restored packet identical to the original packet created by the sending host – Note that such restoration is required because packet header information such as sequence number has been randomized/encrypted before transmission)(col. 7, lines 1-26 and col. 9, lines 30-42), and transmitting each multi-media data flow packet in the re-sequenced series (col. 6, lines 19-67 and col. 7, lines 1-67 and col. 9, lines 13-29).

Regarding claims 46, 53, and 60, Fink discloses wherein said re-sequencing uses a randomization code that is algorithmically predictable if a key to said randomization code (i.e., encryption key) is known (col. 11, lines 29-67 and col. 12, lines 1-6).

Regarding claims 47-49 and 54-56, Fink discloses further comprising the step of performing bit manipulation within said first multi-media data flow packet (col. 9, lines 44-67 and col. 10, lines 1-19).

Regarding claims 50-51, 57-58, and 61-62, Fink discloses the step of pseudo-randomly shuffling (i.e., encrypting using a encryption key) a destination address of

each of the multi-media data flow packets (i.e., the ASD technique seemlessly layers with data security technologies such as IPSEC and Secure Socket Layer (SSL) because it only affects addressing and sequencing information for translation/restoration, allowing it to be used to enhance existing network security systems)(col. 7, lines 1-15 and col. 9, lines 13-65).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 63-67 and 70-73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al., (U.S. Patent No. 6,826,684 and Fink hereinafter), in view of Akiyama et al., (U.S. Patent No. 5,623,548 and Akiyama hereinafter).

Regarding claim 63, Fink discloses a method of encrypting multi-media data flow packets, comprising the steps of:

receiving a series of multi-media data flow packets, each packet comprising a sequence number, storing the series of multi-media data flow packets in a jitter buffer (i.e., for the duration of translation process, packets have to be stored in some sort of buffer or temporary storage)(col. 6, lines 3-60);

re-sequencing (i.e., encrypting) the series of multi-media data flow packets into a pseudo-random order (i.e., the encrypted portions of the packet header are those portions relating to the source and destination hosts 31, and 34 and packet sequencing information ... the receiving ASD peer 35 restores packet in accordance with a prearranged protocol. The result of this process is a restored packet identical to the original packet created by the sending host – Note that such restoration is required because packet header information such as sequence number has been randomized/encrypted before transmission)(col. 7, lines 1-26 and col. 9, lines 30-42), and transmitting each multi-media data flow packet in the re-sequenced series (col. 6, lines 19-67 and col. 7, lines 1-67 and col. 9, lines 13-29).

Fink does not expressly disclose generating a non-duplicating pseudo-random sequence of integers, the sequence containing M integers, each integer between 1 and M, and reordering at least a portion of the bytes of the first packet into a new order specified by the integers in the generated sequence.

However, Akiyama discloses generating a non-duplicating pseudo-random sequence of integers, the sequence containing M integers, each integer between 1 and M, and reordering at least a portion of the bytes of the first packet into a new order specified by the integers in the generated sequence (col. 9, lines 54-67 and col. 10, lines 1-41).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Fink with teachings of Akiyama because it would allow to include generating a non-duplicating pseudo-random

sequence of integers, the sequence containing M integers, each integer between 1 and M, and reordering at least a portion of the bytes of the first packet into a new order specified by the integers in the generated sequence as disclosed by Akiyama. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Akiyama to provide randomization of input data to realize a cryptosystem virtually unbreakable through differential attack (Akiyama, col. 2, lines 45-54).

Regarding claims 64-65, Fink discloses wherein M is equal or less than the maximum size of the first multi-media data flow packet (col. 8, lines 21-35).

Regarding claim 67, Fink discloses a method of encrypting a series of multi-media data flow packets, comprising the steps of:

receiving a series of multi-media data flow packets belonging to a first flow, each packet in the series having the same port address, generating a pseudo-random sequence of numbers (i.e., non-repeating sequence number), the sequence associated with the port address (col. 8, lines 10-45 and col. 9, lines 1-29); and

replacing the port address in each packet with the corresponding number in the sequence (i.e., To overcome keeping the portion of encrypted block from remaining constant, Fink uses exclusive ORing the N-bit unchanging block with the sequence parameter which is changing packet by packet), and transmitting each packet to a receiver (col. 9, lines 50-67).

Moreover, Akiyama discloses replacing the port address in each packet with the corresponding number in the sequence (col. 10, lines 44-67 and col. 11, lines 1-30 and col. 12, lines 1-43).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Fink with teachings of Akiyama because it would allow to include replacing the port address in each packet with the corresponding number in the sequence as disclosed by Akiyama. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Akiyama to provide randomization of input data to realize a cryptosystem virtually unbreakable through differential attack (Akiyama, col. 2, lines 45-54).

Regarding claim 70, Fink discloses wherein the generating step uses a randomization code that is predictable if a key to the randomization code is known (col. 11, lines 15-67 and col. 12, lines 1-27).

Regarding claim 71, Fink discloses wherein the key is known to the receiver (col. 11, lines 15-67 and col. 12, lines 1-27).

Regarding claim 72, Fink discloses wherein the size of the sequence is known to the receiver (col. 10, lines 13-67 and col. 11, lines 1-15).

Regarding claim 73, Fink discloses wherein the port address comprises a destination port address (col. 9, lines 13-30).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Hosford et al., (U.S. Patent No. 5,966,450), and

Eng et al., (U.S. Patent No. 5,457,679).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

A.S.

Patent Examiner
Group 2131
6/15/2006